PPG

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/304,444	05/03/1999	GREGORY BURNS	MS1-301US	9671

22801 7590 07/02/2003

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 07/02/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/304,444	Applicant(s) BURNS ET AL.	
	Examiner Paula W Klimach	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on 10/3/01 .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) 1-19 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other:

DETAILED ACTION

Double Patenting

> The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).
> A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).
> Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

1. Claim 1- 4 provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1, 4, 5, 6, 22 and 26, 22 and 26, 22, 24, and 10 respectively of copending Application No. 9,304,035, the Webster's dictionary, and Microsoft Press Computer Dictionary. Although the conflicting claims are not identical, they are not patentably distinct from each other because:

2. Claim 1 (9304444), differs from claim 1(9304035) because:

- It sites a system for porting user data, while the claim 1 (9304035) sites an assembly. An assembly, is a type of a system, where manufactured parts form a unified whole or a unit of a machine, Webster's dictionary pg 68. The claim 1 (9304444) uses parts of a machine, therefore an assembly as stated in claim 1 (9304035), to port the user data.

- It discusses a system for porting user data from one computer to another, however, claim 1 (9304035) sites a device constructed in a form factor of a PCMCIA card. The PCMCIA card is a common standard and therefore transferable from computer to computer. The PCMCIA card is also a removable device that is primarily a memory-related peripheral, Microsoft Press Computer Dictionary page 357. As a result, the device constructed in the form factor of a PCMCIA card can be used to transfer user data from one computer to another.
- It sites smart card associated with a user, while claim 1 (9304035) sites a removable storage card associated with a user. It is well known in the art that a smart card is a removable device with memory for storing data.
- It teaches both the memory device and the smart card being interfaced with a common computer, while claim 1 (9304035) does not expressly disclose a common computer. The PCMCIA card and the removable storage card of the application 9304035 must be interfaced to the same computer because access to the user data is enabled only when the removable storage card is interfaced with the device interface and disabled when the removable card is removed from the device.

3. Claims 2-4 of 9304444 differ from claims 4-6 respectively of application 9304035 because of the limitation from 2-4 are found in 4-6..

4. Claim 5-10 provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1, 4, 5, 6, 22 and 26, 22 and 26, 22, 24, and 10 respectively of copending Application No. 9,304,035 and the Microsoft Press Computer Dictionary. Although the conflicting claims are not identical, they are not patentably distinct from each other because:

5. Claim 5 and 6 (9304444) differ from claim 26 and 22 (9304035) because:

- Claim 5 (9304444) teaches of a profile carrier, while claim 22 (9304035) teaches of a computer system. The profile carrier carries a user profile, the user profile is a computer based record maintained about an authorized user of a multiuser computer system (Microsoft Computer Dictionary page 588), thus the profile carrier of claim 5 (9304444) is itself a part of a computer system.
- Claim 5 (9304444) sites a memory device to store a user profile, while claim 26 (9304035) sites data memory and does not expressly disclose that the memory is used to store a user profile. However, claim 26 (9304035) inherits from claim 22 (9304035), which teaches that the memory device stores user data. The user profile is data maintained about authorized users (Microsoft Computer Dictionary page 588), and therefore includes user data.
- Claim 5 (9304444) discloses the smart card and the memory device are interfaced with a common computing unit, while claim 26 (9304035) does not expressly disclose this. However, in claim 22 (9304035) the smart card enables access to the user data on the memory device when the card is present

and disables access when the card is absent, therefore, the card and the memory device are interfaced with the same computer.

- Claim 5 (9304444) discloses that the smart card is configured to permit use of the private key following validation of a user-entered passcode. Claim 26 (9304035) discloses that the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key. Since claim 5 (9304444) only permits access to the private key after the validation of a user-entered passcode, then it may be said that the validation is a condition for gaining access to the private key. In claim 26 (9304035) the authentication of the user-supplied passcode means that the passcode goes through validation as a condition for gaining access to the private key (Microsoft Computer dictionary page 36). Therefore both claim 5 (9304444) and claim 26 (9304035) require the passcode is validated before use of the private key is permitted.
- Claim 6 (9304444) does not expressly disclose a computer having a PCMIA device reader as in claim 22 (9304035). However, claim 6 (9304444) does disclose of a memory drive, which is software that permits a computer system to communicate with a device (Microsoft Computer Dictionary page 142). The memory device from claim 5 (9304444) requires a driver in order to access the memory. Therefore claim 22 (9304035) accesses memory and claim 6 (9304444) accesses memory of a specific type, the PCMIA memory device.

- Claim 6 (9304444) discloses a smart card reader, while claim 22 (9304035) discloses a smart card secured memory, therefore the application 9304035 must require a smart card reader to access the information on the smart card for the validation of the memory device and user.
- Claim 6 (9304444) teaches that the memory device is interfaced with the computing unit via the memory drive and the smart card is interfaced with the computing unit via the smart card reader. Claim 22 (9304035) teaches of a smart card secured memory that interfaces with the PCMCIA device reader in the computer. The PCMCIA device reader provides an interface for the computer, by reading PCMCIA cards, (application 9304035, page 5, lines 20-22). It is well known in the art that a computer is a computing device. Therefore the PCMCIA card, which is a memory peripheral (Microsoft Computer Dictionary page 357), is memory that interfaces with the computer through the PCMCIA device reader, which behaves as the driver. Since the memory in the in application 9304035 is smart card secured memory, the application uses a smart card and the interface used for a smart card is the card reader (application 9304035 page 7 lines 21-23)

6. Claim 7 (9304444) differs from claim 22 (9304035) because:

- Claim 7 (9304444) sites a computer having an interface, while claim 22 (9304035) refers to computer having a PCMCIA device reader. The PCMCIA device reader sited in claim 22 (9304035) is an interface between the computer and the computer's PCMCIA slot. The PCMCIA device driver is a specific driver used as an interface for the computer to receive the user data. The interface in claim 7 (9304444) is a general interface for the computer to receive the user's data.

- Claim 7 sites a smart card secured memory system, while claim 22 (9304035) refers to an assembly having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer. An assembly is a type of system of manufactured parts that make up a complete unit, Webster's dictionary pg 68. Therefore, claim 7 (9304444) could describe the system as an assembly. Furthermore the assembly in claim 22 (9304035) having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, is memory that is manufactured to fit in the opening in the housing of a computer (Microsoft Computer dictionary page 395). As a result, the smart card secured memory system sited in claim 7 (9304444) is a general form of memory while the memory in claim 22 (9304035) is a specific type of memory with the dimensions of a PCMCIA slot.

7. Claims 8, 9, and 10 (9304444) differ from claims 24, 25 and 26 (9304035) respectively because of the limitation inherited from claim 7 (9304444) and claim 22 (9304035) whose differences are discussed above.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. **Claim 1 and 7** rejected under 35 U.S.C. 102(e) as being anticipated by Mooney et al 6351813.

In reference to claim 1, the computer system disclosed by Mooney has, in one embodiment, the ability to port data from one computer to another, column 6 lines 31-49. Mooney discloses a memory device to store the user data in column 3 lines 48-51. The computer has a hard drive that is accessed when the computer is accessed; therefore, the system contains memory. Mooney also discloses a smart card in column 3 lines 52-54. The smart card described by Mooney is associated to the user because it is personalized as described in column 7 lines 2-3. The examiner defines the user data as data that is related to the user. The encrypted data in column 3 lines 42-46 is a form of user data because it us protected by a personalized smart card. Since the card is personal to the person encrypting the data, the data is related to the person in possession of the smart card. The encrypted data is stored in the memory, column 3 lines 61-64. The encrypted data is not available to the user unless the user has available to them the keys, which are kept on the smart card, column 3 line 67 to column 4 line 4. Therefore the user does not have access to their data unless both the computer with the data and the smart card are preset.

In reference to claim 7, Mooney discloses a computer system, 100, having an interface to the smart card in the form of and input/output port, 150, and where the computer is secured by the smart card and therefore its memory is secured by a smart card, column 3 lines 48-52. The data on the computer is made accessible by the information stored on the smart card, column 20 lines 0-9. The encrypted data is not available to the user unless the user has available to them the keys, which are kept on the smart card, column 3 line 67 to column 4 line 4. Therefore the user does not have access to their data unless they have the memory device with the data and the smart card.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claim 2, 11, 15, and 16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney as applied to claim 1 above, and further in view of Hayes et al 20010011341

In reference to claim 2, Mooney does not expressly disclose a system wherein the memory device stores a user profile that can be used to configure a computer.

Hayes discloses a user profile that is kept in the user's computer and used to configure the user's computer, page 1 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user's profile described by Hayes in memory device disclosed by Mooney.

One of ordinary skill in the art would have been motivated to do this because user would be required to identify themselves and, therefore gain access permission or not, Hayes page 2 paragraph 12.

In reference to claim 11, Mooney discloses a computer system having a memory drive and a card reader, column 3 lines 48-54. Mooney also discloses an integrated circuit card (smart card) that is associated with the user (column 7 lines 2-3) and that can be interfaced with the computer via the card reader (column 18 lines 13-21). Mooney further discloses a memory device being interfaced with the computer via the memory drive, column 6 lines 40-44 and an IC card that enables access to the user data on the memory device, column 20 lines 0-8.

However, Mooney does not disclose a memory device to store the user's profile.

Hayes discloses a user's profile being stored in memory wherein the profile is accessible to configure the computer (page 1 paragraph 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to save the user's profile described by Hayes in the memory device described by Mooney.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission, Hayes page 2 paragraph 12.

In reference to claim 15, Mooney discloses a computer system that stores user data in memory that is secured by a smart card, column 3 lines 48-54. The smart card selectively enables access to user data in the memory, column 2 lines 21-24.

Mooney does not disclose a system for storing a user's profile for configuring the computer.

Hayes discloses a system where the user's profile is stored in memory for access for configuring the computer, page 1 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile, for configuring the computer that was described by Hayes, in the smart card secured memory system, described by Mooney.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission, Hayes page 2 paragraph 12.

In reference to claim 16, Mooney and Hayes disclose the computer system as applied to claim 15. Mooney further discloses a system where data can be securely transported from one computer to a second computer, column 6 lines 40-44.

11. **Claim 3, 8, and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney as applied to claim1, 7 and 1 respectively above, and further in view of Deo.

In reference to claim 3, Mooney does not expressly disclose a passcode stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card.

Deo discloses a system where the password is stored on the smart card and permits access to the data only when the password that the user enters matches the password stored on the smart card, column 4 lines 66-67 and column 5 lines 1-2. A password, as defined by the Webster's dictionary, is something that enables one to pass or gain admission. Therefore, the pass code is a type of password. The comparing of the password entered by the user with the password stored in the smart card is a form of authenticating the smart card.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode described by Deo on the smart card described by Mooney. One of ordinary skill in the art would have been motivated to do this because the smart cards can perform password verification off-line without connection to a back end computer and are self-validating with the access security code resident thereon, Deo column 2 lines 13-16.

In reference to claim 8, Mooney does not expressly disclose a smart card that has a passcode stored on the smart card.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a password described by Deo on the smart card described by Mooney.

One of ordinary skill in the art would have been motivated to do this because the smart cards can perform password verification off-line without connection to a back end computer and are self-validating with the access security code resident thereon, Deo column 2 lines 13-16.

In reference to claim 17, this claim differs from claim 1 because Mooney does not expressly disclose storing access credentials on a smart card.

Deo teaches of a system where a password (access credential) is stored on the smart card (column 4 lines 66 and 67, column 5 lines 0 and 1) the password is used to enable access to the user data stored on the portable memory device.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to save the access credentials like the password described by Deo on the smart card described by Mooney.

One of ordinary skill in the art would have been motivated to do this because the smart cards can perform password verification off-line without connection to a back end computer and are self-validating with the access security code resident thereon, Deo column 2 lines 13-16.

12. **Claim 4 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney as applied to claim 1 and 7 respectively above, and further in view of Jones et al 5,623,637

In reference to claim 4, Mooney does not disclose a memory device that stores a public key and a smart card that stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated.

Jones discloses, in column 9 lines 25-41, a system where a remote host has a public key for encrypting data and a corresponding smart card has the private key for decrypting data. The data would therefore only be accessible to the computer connected to the smart card, if the smart card possesses the correct private key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key as in Jones on the smart card described by Mooney and a public key as in Jones on the memory device described by Mooney so as to enable the verification of the association of the public key and the private key.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

In reference to claim 9, Mooney does not expressly disclose a public key stored on the memory and a private key stored on the smart card.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key as described by Deo on the smart card described by Mooney and a public key as described by Deo on the memory described by Mooney. One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

13. **Claim 10** rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney as applied to claim 7 above, and further in view of Deo and Jones.

Mooney does not expressly disclose a system where the smart card stores a passcode and a private key of a public/private key pair, with a data memory that stores a public key of the public/private key pair.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key (the second key) and a local device connected to a smart card that contains the private key (the first key), column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. Therefore, acess is allowed only if the keys are corresponding keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the pass code, described by Deo, and private key (the first key), described by Jones on the smart card described by Mooney and to store the public key (the second key) on the memory device described by Mooney.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

14. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney and Hayes as applied to claim 11 above, and further in view of Deo and Jones.

Mooney does not expressly disclose a system where the IC card (smart card) stores a passcode and a private key of a public/private key pair, with a data memory that stores a public key of the public/private key pair.

Deo discloses a password stored on an IC card (smart card), in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the pass code, described by Deo, and private key, described by Jones, on the smart card, described by Mooney, and to store the public key on the memory device, described by Mooney.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

15. **Claim 5 and 6** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Jones, Deo, and Hayes.

In reference to claim 5, Mooney discloses a system comprising of a smart card and a memory device, column 47-52. Mooney also discloses a system where the smart card is configured to permit use of the private key following validation of a user-entered passcode.

Mooney does not disclose a system where the smart card stores a passcode and a private key from a private/public key pair. Mooney further does not disclose a user profile and a public key stored on the memory device. Mooney does not expressly disclose the memory device and the smart card being interface with a common computing unit or authentication of a public key stored on the memory device using the private key and then permitting access to the user data only on the successful authentication of the public key.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. In addition, Jones teaches the smart card and the memory device interfacing with a common computer, fig 2 (The smart card is an integral part of the memory device).

Hayes discloses a user profile that is stored on a computer.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode, described by Deo, and the private key, described by Jones, on the smart card, described by Mooney., to store the user profile and the public key on the computer hard drive, to interface the smart card and the memory device with a common computer, authentication of a public key stored in the memory device before accessing the user data. One of ordinary skill in the art would have been motivated to do this because when the passcode is stored on the smart card the card can perform password verification off-line without connection to a back end computer and smart cards are self-validating with access security code resident thereon, Deo column 2 lines 13-16. Storing the private key on the smart card and the public key on the memory device increases security of the memory device, Jones column 9 lines 55-60.

In reference to claim 6, Mooney discloses a system comprising of a smart card and a memory device, column 47-52. Mooney also discloses a system where the smart card is configured to permit use of the private key following validation of a user-entered passcode. Mooney also discloses a system with a smart card reader and a hard drive. The hard drive is interfaced with the computer and the smart card is interfaced with the computer via the smart card reader.

Mooney does not disclose a system where the smart card stores a passcode and a private key from a private/public key pair. Mooney further does not disclose a user profile and a public key stored on the memory device. Mooney does not expressly disclose the memory device and the smart card being interface with a common computing unit or authentication of a public key stored on the memory device using the private key and then permitting access to the user data only on the successful authentication of the public key.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. In addition, Jones teaches the smart card and the memory device interfacing with a common computer, fig 2 (The smart card is an integral part of the memory device).

Hayes discloses a user profile that is stored on a computer.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode and the private key on the smart card, to store the user profile and the public key on the computer hard drive, to interface the smart card and the memory device with a common computer, authentication of a public key stored in the memory device before accessing the user data. One of ordinary skill in the art would have been motivated to do this because the smart card with password, security system prevents access of unauthorized users while enabling the authorized user quick access data, Deo column 3 lines 4-6, where the data stored in this case would be the user profile. It would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

16. **Claim 12** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney and Hayes in view of Deo.

Mooney and Hayes disclose a computer system as applied to claim 11.

Mooney does not expressly disclose an IC card (smart card) that stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile.

Deo discloses a smart card that stores the password and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile, column 2 lines 66-67 and column 5 lines 1-2.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the password in the smart card and configure it to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile. One of ordinary skill in the art would have been motivated to do this because the security system prevents access of an unauthorized user while enabling the authorized user quick access, Deo column 3 lines 4-6.

17. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney and Hayes in view of Jones.

Mooney and Hayes disclose a computer system as applied to claim 11.

Neither Mooney nor Hayes expressly discloses a public key stored on the memory and a private key stored on the smart card.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key on the smart card and a public key on the memory. One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

18. **Claim 18** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Deo, Jones, SigbjØrnsen et al US 6,266,416 B1, and Kutler.

Mooney discloses a system that stores user data in a portable memory device, column 6 lines 43 and 44; a computer that interfaces with a smart card, column 3 lines 48-54; a portable memory device that interfaces with the computer, column 3 lines 61-64; user-entered password, column 4 lines 2-4; and use of the card resident key permitted only after validation of the user entered password, column 4 lines 2-4.

Mooney does not expressly disclose a system where the a key is stored on the memory device the corresponding key is stored on the smart card, storing a passcode on the smart card, passing the key from the memory device to the smart card, and authenticating the at the smart card using the card resident key.

Deo discloses password stored on a smart card (column 4 lines 66 and 67, column 5 lines 0 and 1).

Jones discloses a system where a key is stored on a remote device (the memory device) and a corresponding key is stored on the local device (the smart card), column 9 lines 24-42.

SigbjØrnsen teaches of a system where an asymmetric authentication key is transferred to the smart card and decrypted in the smart card to initiate an authentication process in the smart card, column 7 lines 44-49.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art would use the system to store the password and a key on the smart card, store a corresponding key on the memory device, and transmitting the stored key from the memory device to the smart card in order to carryout the authentication.

One of ordinary skill in the art would have been motivated to do this because storing the password and a key on the smart card and a corresponding key on the memory device would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60. Carrying out authentication on the smart card give the users complete portability, user authentication can be carried out across operating systems and multiple computers, Kutler, page 13, paragraph 4.

19. **Claim 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney in view of Hayes, Deo, and Jones.

Mooney discloses a system with a smart card secured memory, column 3 lines 48-55. The system receives a user-supplied password from the computer, column 4 lines 2-4, and enables access to the private key on the smart card upon successful authentication of the user-supplied password Mooney column 4 lines 2-4.

Mooney does not expressly disclose the user profile stored on the memory device, a password stored on the smart card, and public key and private keys stored on the smart card and the memory device.

Hayes discloses a system where the user profile is stored in memory for the configuration of the computer, page 1 paragraph 4.

Deo discloses a smart card that has a password stored on the smart card (column 4 lines 66 and 67, column 5 lines 0 and 1).

Jones discloses a system where the public key is stored on remote computer (memory device) and a private key stored in host computer (smart card), column 9 lines 24-42.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile on the memory device, store the password on the smart card and store corresponding keys on the smart card and the memory device.

One of ordinary skill in the art would have been motivated to do this because storing the password and a key on the smart card and a corresponding key on the memory device would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Mooney et al	6,351,813 B1
Deo	5,594,227
Jones et al	5,623,637
Hayes et al	2001/0011341 A1
Sigbjørnsen et al	6,266,416 B1
Kutler	

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-8421 for regular communications and (703) 305-8421 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
June 25, 2003

Gail Hay

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100